Hacking my children's toys...

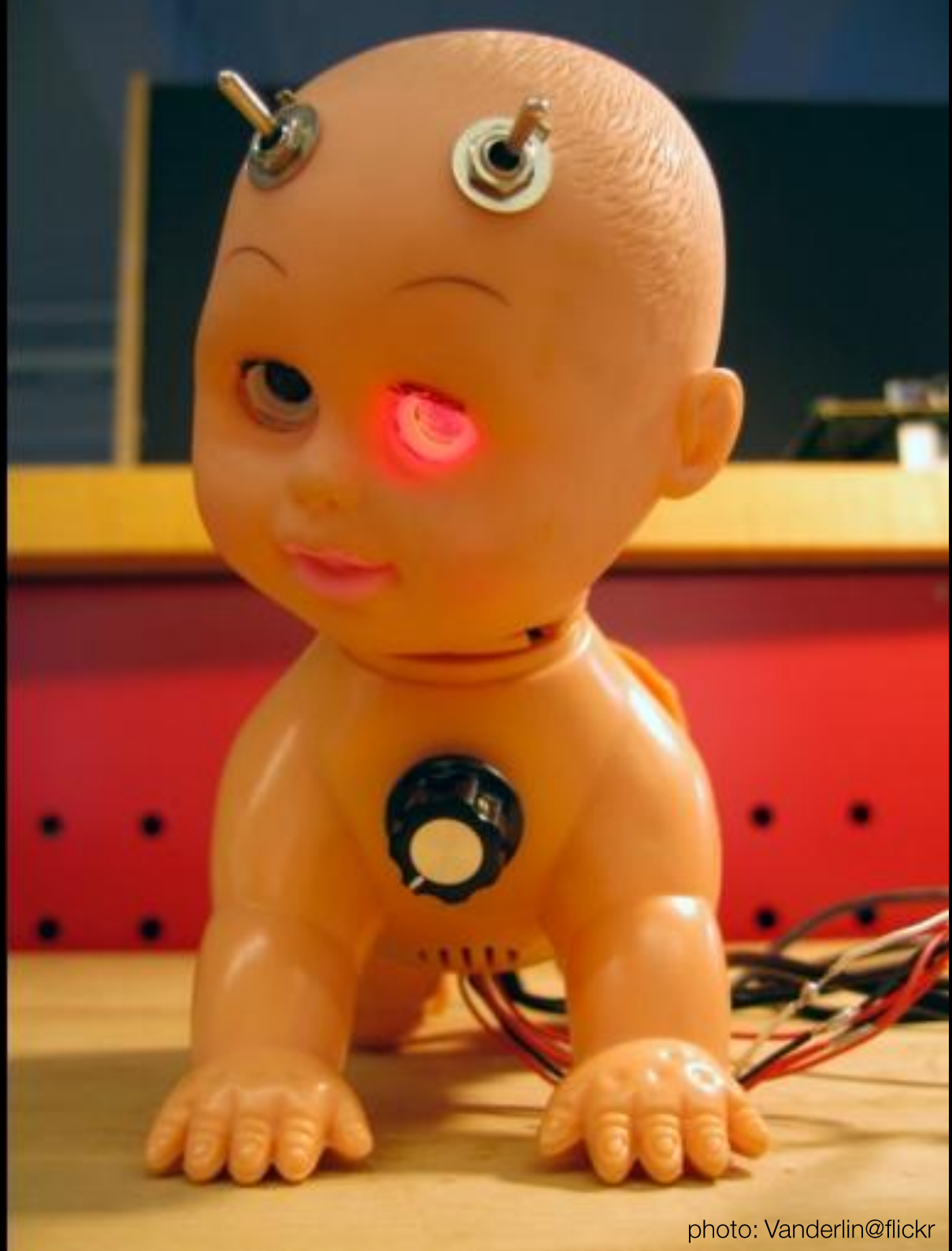


photo: Vanderlin@flickr

Why do this?

Because you can.

You can do something with a product or a piece of hardware that has never been done before.

You can create something extraordinary.

You harm nobody in the process.

- Joe Grand

Under the knife today...

Leapster Explorer (aka LX)

Didj

Feeds and Speeds:

LF1000 (aka Pollux)
ARM 926EJ-S – 393MHz

32 (Didj) or 64MB (LX) SDRAM
256 (Didj) or 512MB (LX) NAND

USB Host
(LX – via Accessory port)
USB Device
(Didj/LX)

Research: Get datasheets.

Key facets of the LF1000 CPU as revealed in the datasheets:

1. Embedded Serial I/O (UART)
2. Ability to boot from UARTT
3. Onboard USB, I2C, SPI
4. Composite TV Out***

Get the datasheets.
(Google is your friend!)


Explorer
LeapFrog


42
6 x 7 = ?
didj

Research: Get source.

Next,investigate the interfaces:

Look for ways in…

Tools:
Multimeter
Soldering Iron (be not afraid!)
A few electronic components

…and your powers of observation.

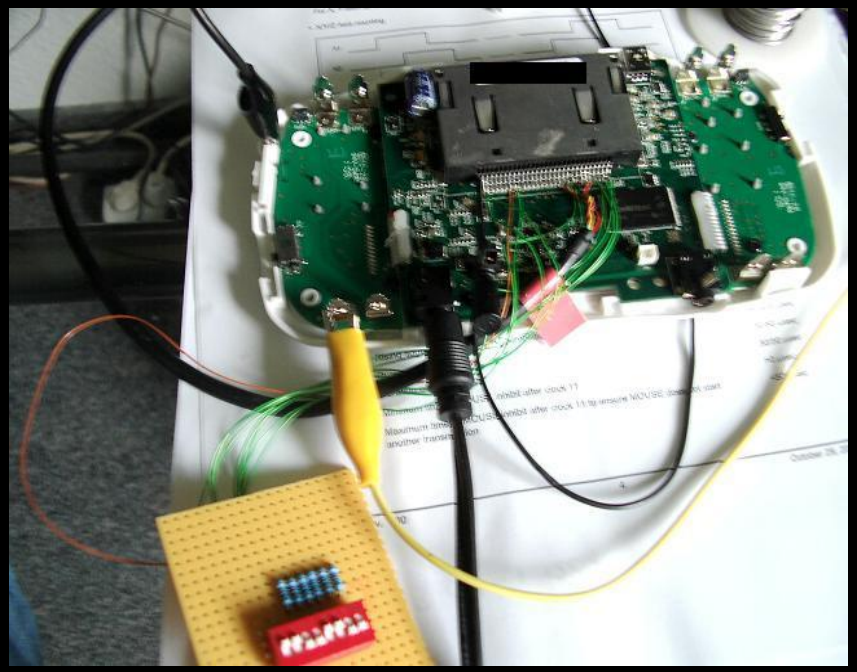
Ways in…

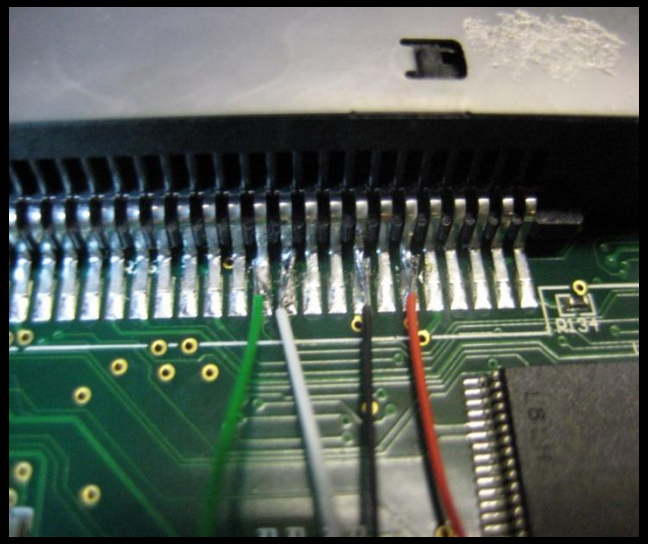
Cartridge Socket

USB

Ways in:

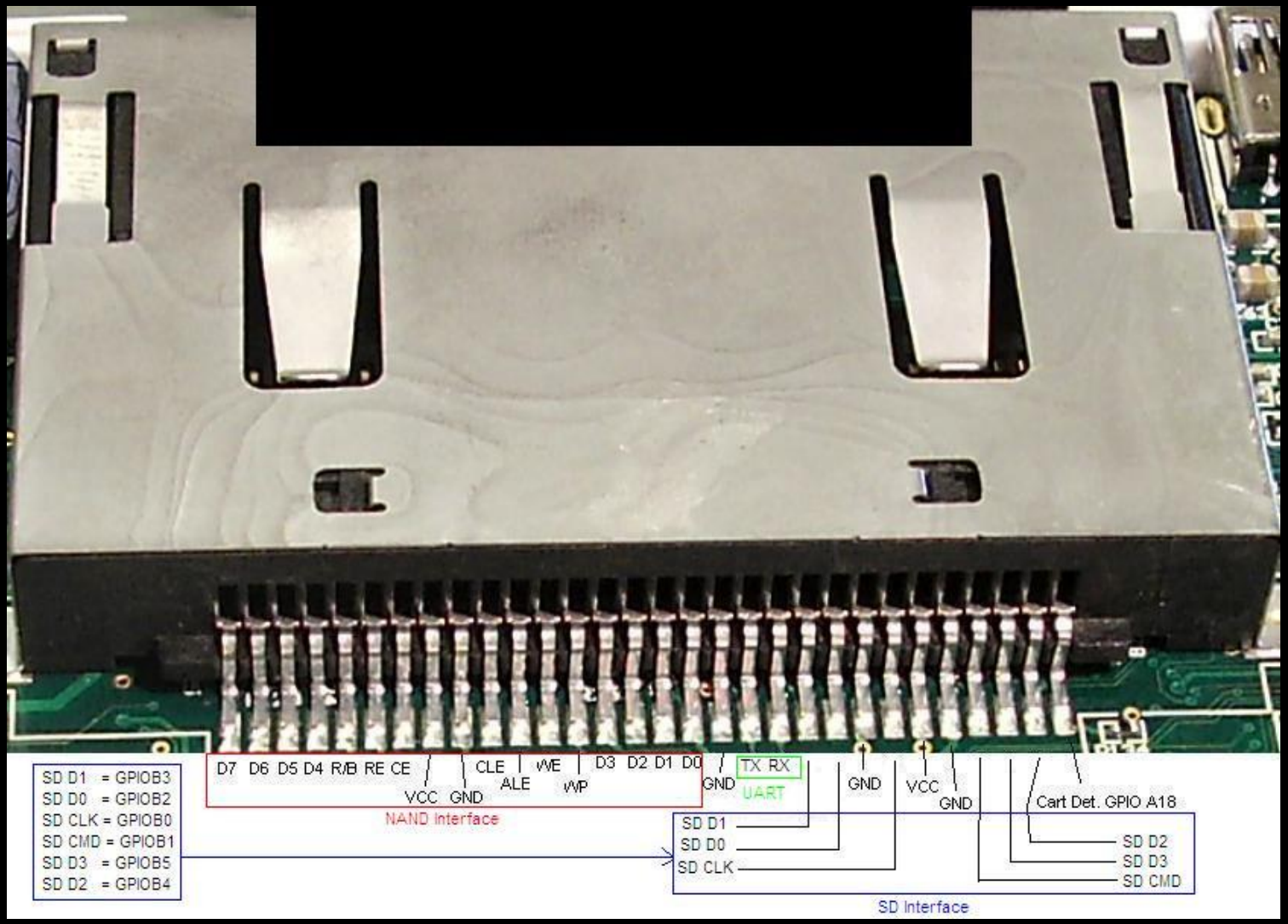
The Cart Socket…





Bingo! 115200 8N1 (yay!)

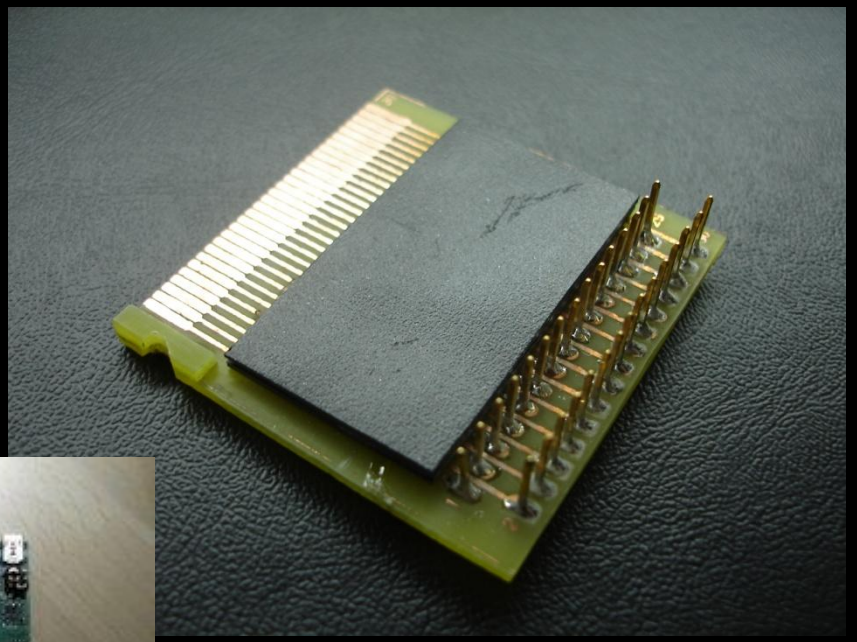
photos: claude

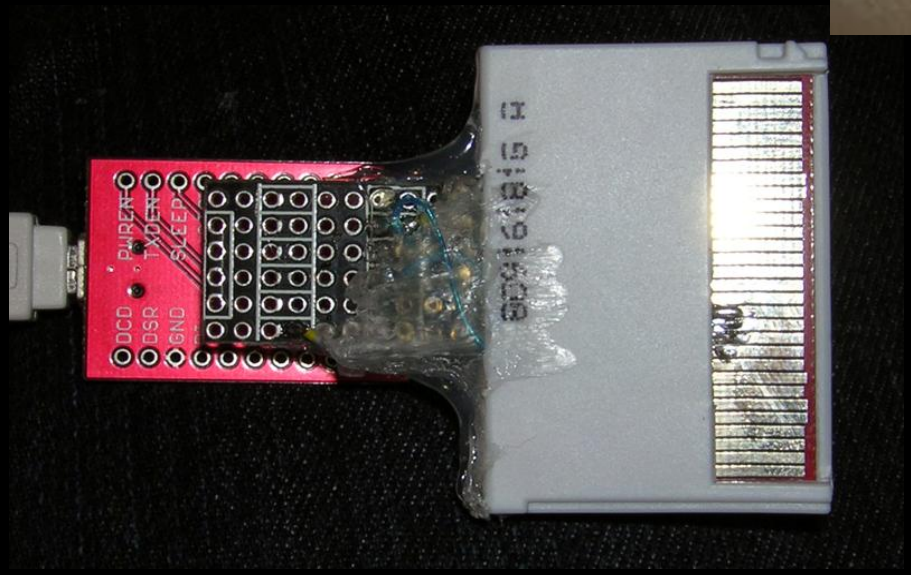


What was found? Serial, SDIO, NAND (ex. xD)

photo: claude

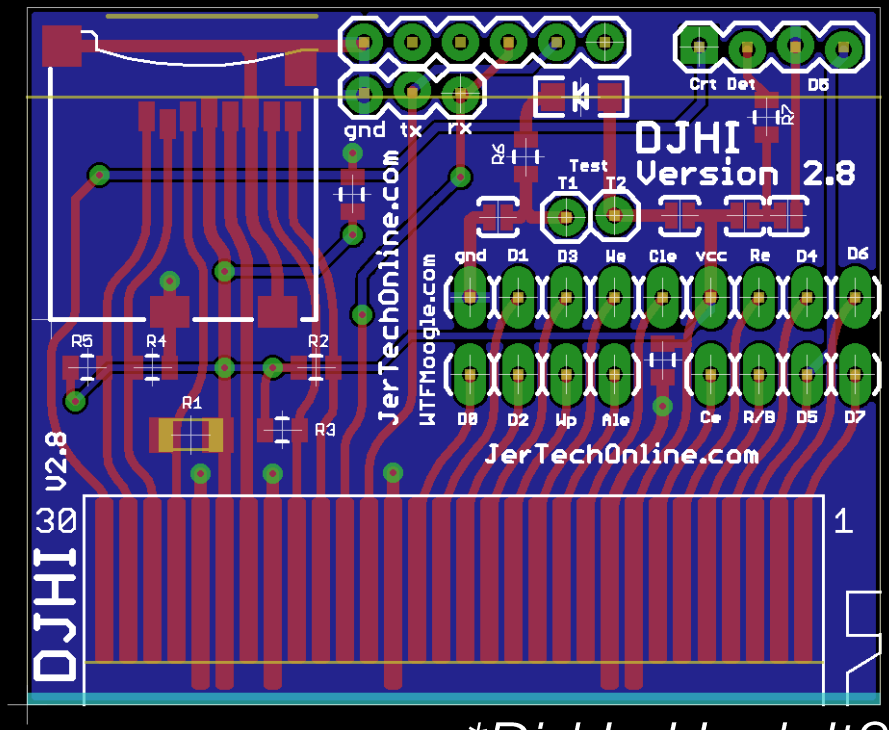
A rogue's gallery of homebrew breakout boards:





photos: moogle, claude, awesomneser

The first hacker-developed product, the DJHI*:



*DidJa Hack It?

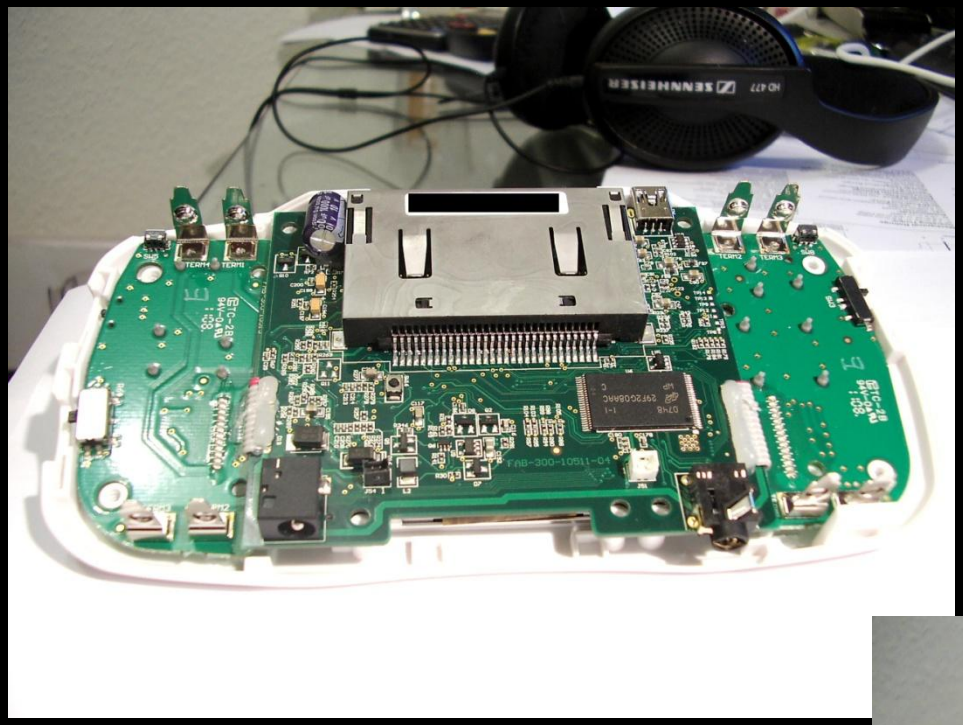
diagram: moogle

Demo: Got Root? (on a toy!)

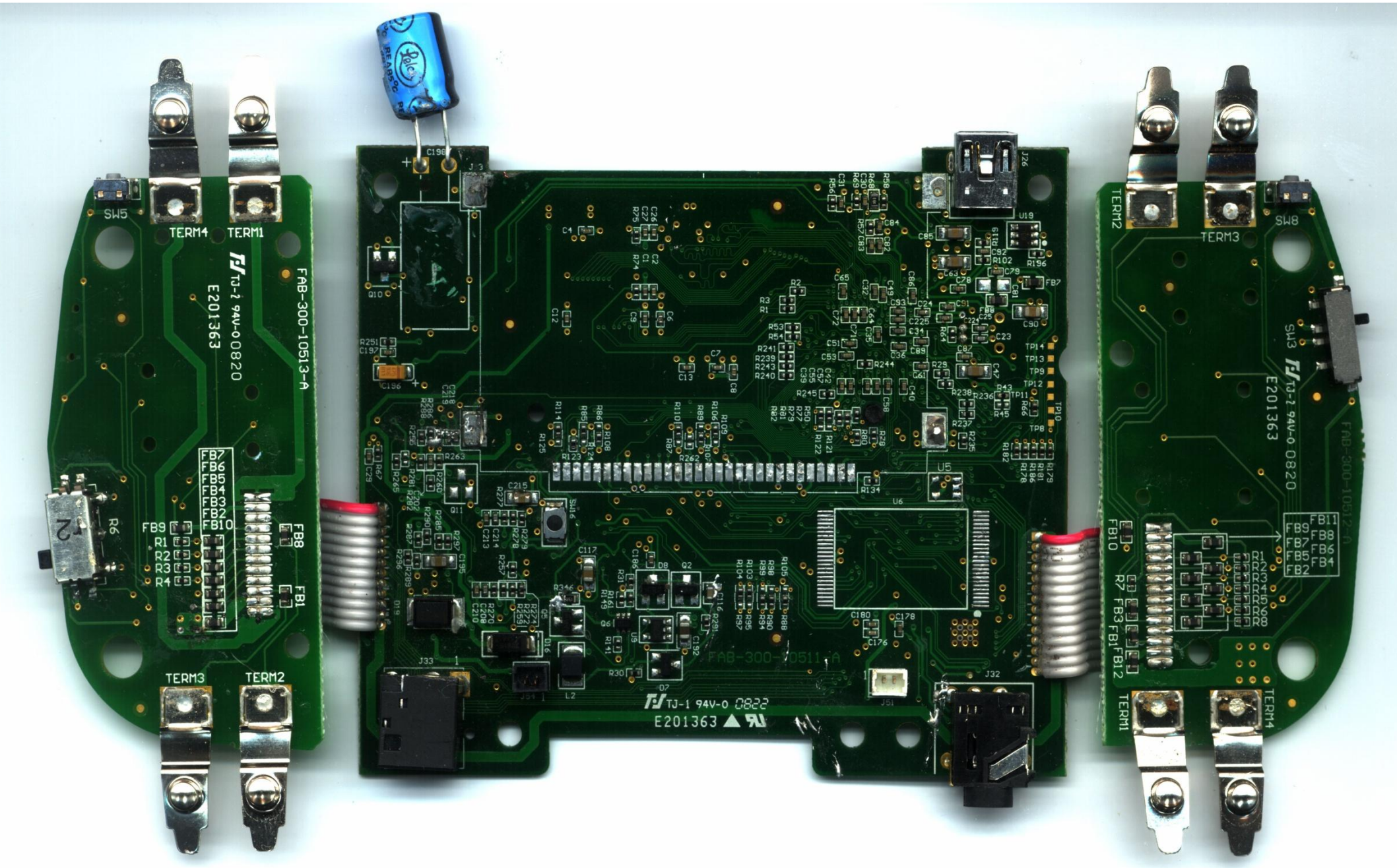
Demo: Taking control...UART Boot.
(Remember the datasheet?)

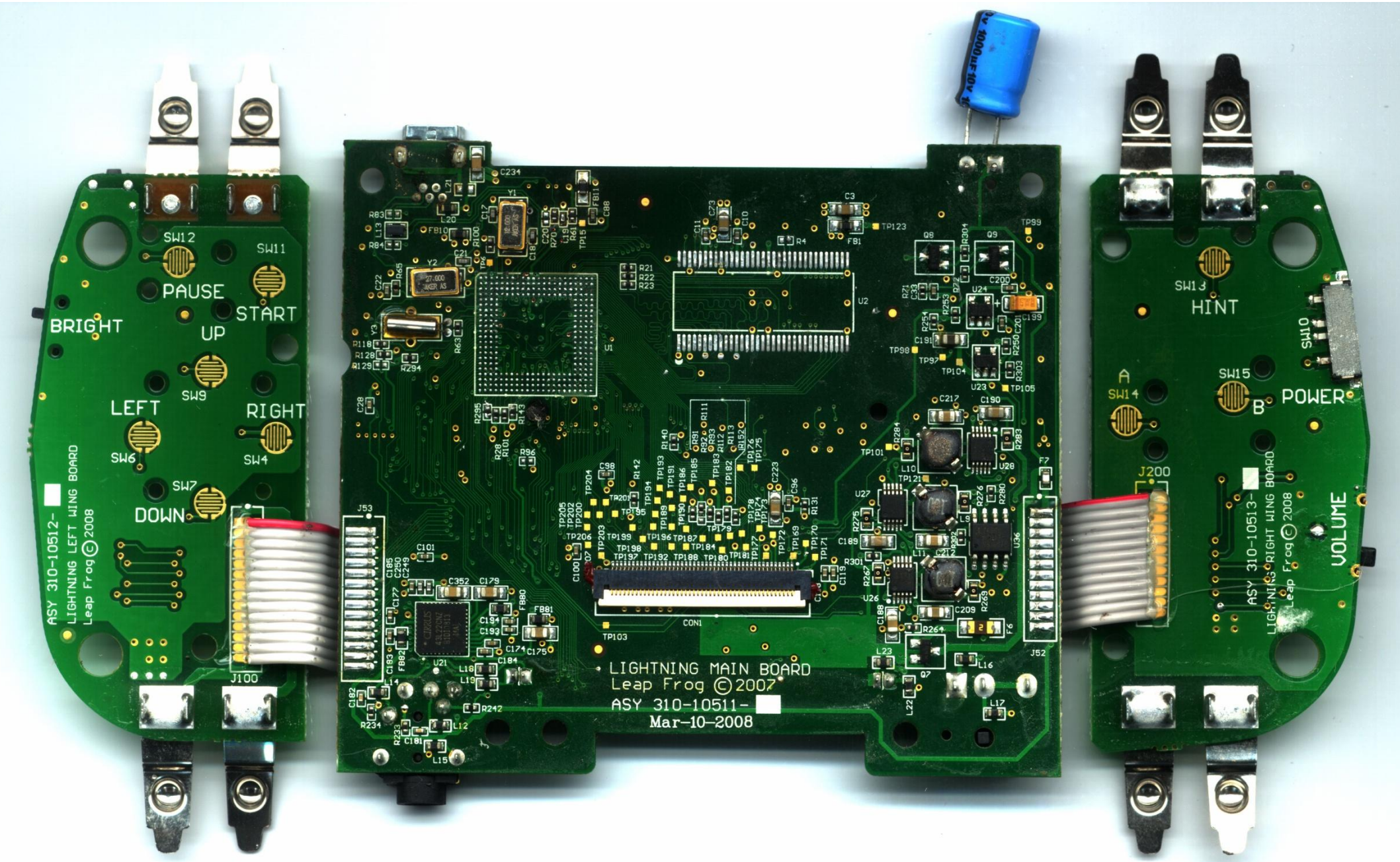
Deeper investigation: Reversing the hardware.

Tools:
Flatbed scanner
Stereo microscope (or a USB microscope.)
Heatgun (or a hot-air SMD rework station)
Multimeter
JTAG dongle
Datasheet

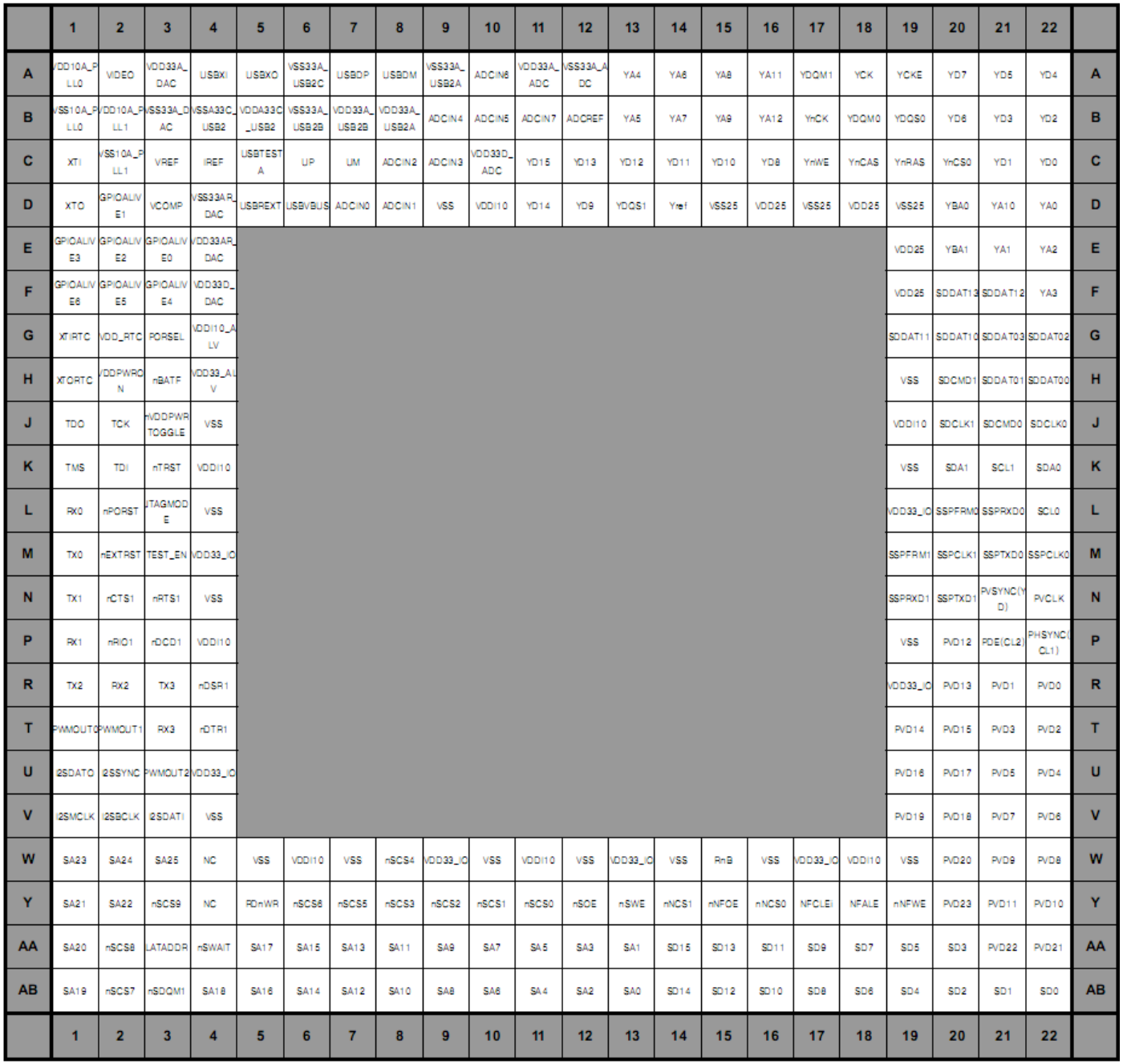


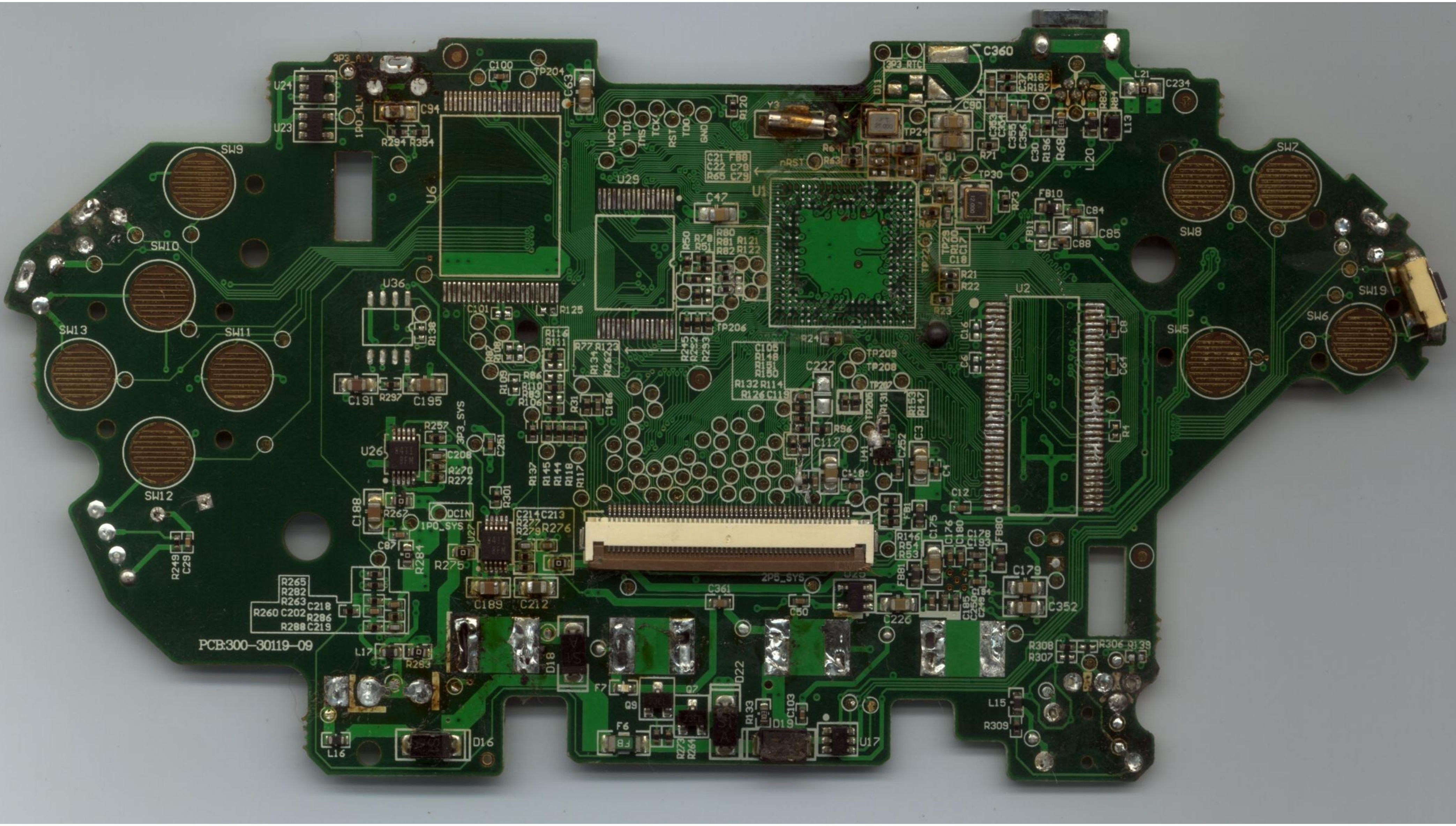
photos: claude


SW5
TERM4
TERM1
TERM3
TERM2
FAB-300-10513-A
TJ-1 94V-0 0820
E201363
FB7
FB6
FB5
FB4
FB3
FB2
FB10
FB9
FB8
FB1
R1
R2
R3
R4
R6
TJ-1 94V-0 0822
E201363
SW8
TERM2
TERM3
TERM1
TERM4
SW3
FB11
FB9
FB8
FB7
FB6
FB5
FB4
FB2
FB10
R7
FB3
FB1
FB12


SW12
SW11
PAUSE
START
BRIGHT
UP
SW9
LEFT
RIGHT
SW6
SW4
SW7
DOWN
ASY 310-10512-
LIGHTNING LEFT WING BOARD
Leap Frog © 2008
J100
J53
CON1
LIGHTNING MAIN BOARD
Leap Frog ©2007
ASY 310-10511-
Mar-10-2008
SW13
HINT
SW10
SW15
POWER
A
SW14
B
J200
VOLUME
ASY 310-10513-
LIGHTNING RIGHT WING BOARD
Leap Frog © 2008
J52

TP6
U1





PCB:300-30119-09
C360
SW7
SW8
SW9
SW10
SW11
SW12
SW13
SW5
SW6
SW19
U1
U2
U6
U29
U36
U26
U24
U23
U17
D16
D18
D19
Y1
Y3
DCIN
VCC
TDI
TMS
TCK
RST
TDO
GND

Discoveries: TV, SPI, JTAG, Audio…

Deeper investigation: Use the Source!

Development:
Tools: Source code. IDE. Cross compiler.

Development:
Framebuffer device
SDL

Demo: Combining what we learned. TV, Emu

Methods Recap:

- Get Datasheets
- Get Source
- Look for ways in.
- Reverse the hardware.
- Use the source.

Tools Recap:

- Multimeter
- Oscilloscope – nice to have.
- Soldering Iron (really, its easy)
- Hookup wire
- Basic electronics
- Heatgun
- Brain (one or more)

elinux.org/Didj
elinux.org/Leapster_Explorer

rosincore.com
irc.freenode.org #Didj
nick: nirvous
hackaday.com/?s=nirvous